Attorney Docket No. 826.1930

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Shinji KIKUCHI et al.

Application No.: Unassigned | Group Art Unit: Unassigned

Filed: (Concurrently) | Examiner: Unassigned

For: DEVICE FOR DETECTING FAILURE OF COMMUNICATION NETWORK

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Application No. 2003-296768

Filed: August 20, 2003

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 3/10/04

By: Richard A. Gollhofer
Richard A. Gollhofer
Registration No. 341,106

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

JAPAN PATENT OFFICE

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: August 20, 2003

Application Number: Patent Application No. 2003-296768
[ST.10/C]: [JP2003-296768]

Applicant(s) : FUJITSU LIMITED

December 22, 2003

Commissioner,
JAPAN Patent Office Yasuo IMAI

Certificate No. P2003-3106430

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　８月２０日

出願番号
Application Number: 特願２００３－２９６７６８

[ST. 10/C]: ［ＪＰ２００３－２９６７６８］

出願人
Applicant(s): 富士通株式会社

２００３年１２月２２日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３１０６４３０

【書類名】　特許願
【整理番号】　0351810
【提出日】　平成15年 8月20日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 17/00
H04L 12/26
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　菊池　慎司
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　中原　浩之
【特許出願人】
【識別番号】　000005223
【氏名又は名称】　富士通株式会社
【代理人】
【識別番号】　100074099
【住所又は居所】　東京都千代田区二番町８番地２０　二番町ビル３Ｆ
【弁理士】
【氏名又は名称】　大菅　義之
【電話番号】　03-3238-0031
【選任した代理人】
【識別番号】　100067987
【住所又は居所】　神奈川県横浜市鶴見区北寺尾７－２５－２８－５０３
【弁理士】
【氏名又は名称】　久木元　彰
【電話番号】　045-545-9280
【手数料の表示】
【予納台帳番号】　012542
【納付金額】　21,000円
【提出物件の目録】
【物件名】　特許請求の範囲　1
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9705047

【書類名】特許請求の範囲
【請求項１】
複数の通信インタフェースを有し通信ネットワーク内に配置された監視対象機器から得られる情報に基づいて、ネットワーク障害を検出する障害検出装置であって、
前記監視対象機器の各インタフェースにおける受信トラフィック量と送信トラフィック量を表すトラフィック流量情報を格納する格納手段と、
前記トラフィック流量情報を用いて、前記監視対象機器の内部における複数のトラフィックのうち異常なトラフィックの流量を計算し、得られた流量を異常トラフィック量として出力する計算手段と、
前記異常トラフィック量を用いて前記ネットワーク障害が発生したか否かを判定し、判定結果を出力する判定手段と
を備えることを特徴とする障害検出装置。
【請求項２】
複数の通信インタフェースを有し通信ネットワーク内に配置された監視対象機器から得られる情報に基づいて、ネットワーク障害を検出するコンピュータのためのプログラムであって、
前記コンピュータの格納手段から、前記監視対象機器の各インタフェースにおける受信トラフィック量と送信トラフィック量を表すトラフィック流量情報を取り出し、
前記トラフィック流量情報を用いて、前記監視対象機器の内部における複数のトラフィックのうち異常なトラフィックの流量を計算し、
得られた流量を異常トラフィック量として用いて前記ネットワーク障害が発生したか否かを判定する
処理を前記コンピュータに実行させることを特徴とするプログラム。
【請求項３】
前記監視対象機器により生成されて出力されるデータのトラフィック量と、該監視対象機器により廃棄されるデータのトラフィック量と、該監視対象機器のインタフェースにより受信された後に同じインタフェースから送信されるデータのトラフィック量のうち少なくとも１つのトラフィック量を、前記異常トラフィック量として計算する処理を前記コンピュータに実行させることを特徴とする請求項２記載のプログラム。
【請求項４】
前記監視対象機器の内部におけるトラフィックの総量に対する前記異常トラフィック量の比率を求め、該異常トラフィック量の比率が所定の閾値より大きい場合に前記ネットワーク障害が発生したと判定する処理を前記コンピュータに実行させることを特徴とする請求項２記載のプログラム。
【請求項５】
前記監視対象機器の内部にトラフィックの終点および始点を表す仮想点を設け、該監視対象機器の内部において各インタフェースを始点とし他のインタフェースを終点とする第１のトラフィックの流量と、各インタフェースを始点とし該仮想点を終点とする第２のトラフィックの流量と、該仮想点を始点とし各インタフェースを終点とする第３のトラフィックの流量と、該監視対象機器の内部において各インタフェースを始点とし同じインタフェースを終点とする第４のトラフィックの流量を計算し、該第２、第３、および第４のトラフィックの流量の総量を前記異常トラフィック量として計算する処理を前記コンピュータに実行させることを特徴とする請求項２記載のプログラム。

【書類名】明細書
【発明の名称】通信ネットワークの障害を検出する装置
【技術分野】
【０００１】
本発明は、通信ネットワークにおけるトラフィックの流れを解析することによりネットワークの障害を検出する装置に関する。
【背景技術】
【０００２】
従来より、通信ネットワーク内の障害を検知するための技術としては、以下のようなものが知られている。
（Ａ）エラーメッセージ捕捉
監視機器は、障害発生時にネットワーク機器が生成するエラーメッセージを観測し、生成されたエラーメッセージを捕捉したらアラームを出力して、ネットワーク管理者に障害の発生を通知する（例えば、非特許文献１参照）。
（Ｂ）パケットキャプチャ
ネットワーク内部に流れるパケットを捕捉し、それらのパケットを１つ１つ調査することにより、障害が発生しているかどうかを判定する（例えば、非特許文献２参照）。
【０００３】
また、トラフィック行列（Traffic Matrix）を用いたいくつかのネットワーク解析方法も知られている（例えば、非特許文献３および４参照）。
【０００４】
【非特許文献１】“Remote Network Monitoring Management Information Base”、[online]、ＲＦＣ　１７５７、[平成１５年７月１８日検索]、インターネット<ＵＲＬ：http://www.faqs.org/rfcs/rfc1757.html>
【非特許文献２】“Sniffer Technologies（登録商標）”、[online]、Network Associates、[平成１５年７月１８日検索]、インターネット<ＵＲＬ：http://www.nai.com/japan/products/sniffer/home.asp>
【非特許文献３】J. Cao, D. Davis, S. Vander Wiel, and B. Yu, "Time-Varying Network Tomography: Router Link Data", Journal of the American Statistical Association, 2000
【非特許文献４】C. Tebaldi and M. West, "Bayesian Inference on Network Traffic Using Link Count Data", Journal of the American Statistical Association, 1998
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、上述した従来の障害検出方法には、次のような問題がある。
【０００６】
上記（Ａ）の方法においては、例えばＩＰ（Internet Protocol）ネットワークにおけるICMP(Internet Control Message Protocol) destination unreachable エラーや、ICMP time exceededエラーを観測し、それらのエラーメッセージの発生の有無に基づいて障害の存在を確認する。
【０００７】
しかし、これらのエラーメッセージを発生させない障害も多数存在する。また、これらのエラーメッセージは、ユーザによる経路調査ツールtracerouteの実行や、アクセス時の宛先ＩＰアドレスの指定ミス等により、ネットワーク内に定常的に存在する。このようなことから、障害の程度が小さい場合には、これらのエラーメッセージの発生頻度も小さいため、これらのエラーメッセージの有無に基づいて障害の検知を行うのは一般的には困難である。
【０００８】

また、上記（Ｂ）の方法においては、パケットキャプチャ機器を、障害が原因で発生するパケットが流れる場所に配置しなければならないため、広い範囲のネットワークを監視する場合、多数のパケットキャプチャ機器を配置する必要がある。また、全てのパケットデータを高速に大量に記録する必要があるため、そのためのリソース消費は多大である。このようなことから、パケットキャプチャを用いた障害検出方法はコストが非常に高くなるため、現実的な方法であるとは言えない。

【０００９】

本発明の課題は、通信ネットワーク内で発生する障害を、その影響が比較的小さい早期のうちに低コストで検出する障害検出装置を提供することである。

【課題を解決するための手段】

【００１０】

図１は、本発明の障害検出装置の原理図である。図１の障害検出装置は、格納手段１０１、計算手段１０２、および判定手段１０３を備え、複数の通信インタフェースを有し通信ネットワーク内に配置された監視対象機器から得られる情報に基づいて、ネットワーク障害を検出する。

【００１１】

格納手段１０１は、監視対象機器の各インタフェースにおける受信トラフィック量と送信トラフィック量を表すトラフィック流量情報を格納する。計算手段１０２は、トラフィック流量情報を用いて、監視対象機器の内部における複数のトラフィックのうち異常なトラフィックの流量を計算し、得られた流量を異常トラフィック量として出力する。判定手段１０３は、異常トラフィック量を用いてネットワーク障害が発生したか否かを判定し、判定結果を出力する。

【００１２】

格納手段１０１は、例えば、後述する図３のトラフィック流量記録装置３１２および後述する図８のトラフィック流量記録装置８０１に対応する。計算手段１０２は、例えば、図３のトラフィック流量分析装置３１３および異常トラフィック量計算装置３１４と、図８のトラフィック流量分析装置８０２および異常トラフィック量計算装置８０３に対応する。判定手段１０３は、例えば、図３の障害判定装置３１５および図８の障害判定装置８０４に対応する。

【発明の効果】

【００１３】

本発明によれば、容易に取得可能なトラフィック流量情報を分析し、そこから異常な流れ方をするトラフィックの量を導出することにより、ネットワーク障害の有無が判定される。これにより、ネットワーク内で発生するエラーメッセージに頼ることなく、またネットワーク内に特別なパケットキャプチャ機器を配置することなく、ネットワーク内部を流れる異常トラフィックを識別することができる。したがって、広範囲な通信ネットワークにおいて、障害の影響が小さいうちに、その障害の発生を早期にかつ低コストで検出することが可能になる。

【発明を実施するための最良の形態】

【００１４】

以下、図面を参照しながら、本発明を実施するための最良の形態を詳細に説明する。

【００１５】

図２は、本発明を実施するためのネットワーク構成の例を示している。図２のネットワーク構成において、障害検出装置２０１は、通信ネットワーク内部における複数の中継機器等の監視対象機器２０２～２０７からトラフィック流量情報を収集し、それらの監視対象機器における障害の有無を判断する。ここでは、簡単のため６つの監視対象機器が示されているが、監視対象機器の数は一般に任意である。

【００１６】

障害検出装置２０１は、図３に示すように、トラフィック流量取得装置３１１、トラフィック流量記録装置３１２、トラフィック流量分析装置３１３、異常トラフィック量計算

装置３１４、および障害判定装置３１５を備え、ネットワーク内部の障害を検出する。監視対象機器３０１は、図２の監視対象機器２０２～２０７のいずれかに対応する。

【００１７】

図４は、図３の障害検出装置２０１による障害検出処理のフローチャートである。図４の障害検出処理の手順は、以下のようになる。

ステップ４０１：

トラフィック流量取得装置３１１は、監視対象機器３０１に対して、その監視対象機器３０１が保持しているトラフィック流量情報を要求するリクエストを送信する。そのリクエストに対して、監視対象機器３０１は、それが保持しているトラフィック流量情報を障害検出装置２０１に対して送信する。例えば、ＩＰネットワークの場合、このトラフィック流量情報としては、監視対象機器３０１のManagement Information Base-II（ＭＩＢ－ＩＩ）データベースに保持されている、各インタフェースにおける入力／出力パケット数や、入力／出力オクテット数等が用いられる。また、トラフィック流量取得装置３１１が送出するリクエストとしては、Simple Network Management Protocol（ＳＮＭＰ）のgetリクエスト等が用いられる。

ステップ４０２：

トラフィック流量取得装置３１１が監視対象機器３０１のトラフィック流量情報を取得すると、トラフィック流量記録装置３１２は、その流量情報を記録する。

ステップ４０３：

トラフィック流量分析装置３１３は、記録されたトラフィック流量情報を用いて、トラフィック流量の分析を行う。ここで行われる分析とは、ネットワーク内を流れる個々のパケットの保持するデータや挙動を調査するのではなく、トラフィックの大局的な流れを捉えることを言う。例えば、トラフィックが監視対象機器３０１のどのインタフェースから入力され、そのトラフィックがどのインタフェースから出力されるかを、各インタフェースにおけるトラフィック流量情報から推定する。

【００１８】

例えば、監視対象機器３０１が３つのインタフェースを持つルータである場合、このルータは図５のようなモデルにより表現できる。このモデルにおいては、ルータは３つのインタフェースＡ、Ｂ、およびＣを持ち、それぞれのインタフェースにおける単位時間当たりの受信トラフィック量（y_{in-A}, y_{in-B}, y_{in-C}）と送信トラフィック量（y_{out-A}, y_{out-B}, y_{out-C}）が取得可能なトラフィック流量情報であるとする。

【００１９】

また、ルータの内部には、ルータの内部で消滅するトラフィックの終点や、ルータが送信元となるようなトラフィックの始点に対応する仮想的な点を表す要素Ｏがあるものとする。さらに、ルータの内部において、α（$\alpha \in \{A, B, C, O\}$）を始点とし$\beta$（$\beta \in \{A, B, C, O\}$）を終点として流れるトラフィックの量を$x_{\alpha\beta}$と記し、このルータで送受信される全てのトラフィックはいずれかの$x_{\alpha\beta}$にカウントされるものとする。この場合、以下のような連立方程式が成り立つ。

【００２０】

【数１】

$$Y = \begin{pmatrix} y_{in-A} \\ y_{in-B} \\ y_{in-C} \\ y_{out-A} \\ y_{out-B} \\ y_{out-C} \end{pmatrix} \quad (1)$$

$$X = \begin{pmatrix} x_{AA} \\ x_{AB} \\ x_{AC} \\ x_{BA} \\ x_{BB} \\ x_{BC} \\ x_{CA} \\ x_{CB} \\ x_{CC} \\ x_{AO} \\ x_{BO} \\ x_{CO} \\ x_{OA} \\ x_{OB} \\ x_{OC} \end{pmatrix} \quad (2)$$

$$A = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad (3)$$

$$Y = AX \quad (4)$$

【００２１】

しかし、（４）式では、６個の方程式に対して、ルータ内部におけるトラフィックの流れを表す１５個の未知数ｘα βが存在するので、この連立方程式を解析的に解くことはできない。そこで、トラフィック流量分析装置３１３は、単位時間当たりの受信トラフィック量（y_{in-A}, y_{in-B}, y_{in-C}）と送信トラフィック量（y_{out-A}, y_{out-B}, y_{out-C}）から各ｘα βの値を推定する。この推定には、例えば、前述した非特許文献３および４に示されているようなTraffic Matrix Estimation という方法を用いることができる。

ステップ４０４：

トラフィック流量分析装置３１３が監視対象機器３０１の各インタフェース間を流れるトラフィックを推定すると、異常トラフィック量計算装置３１４は、得られたトラフィックのうち監視対象機器３０１の目的にそぐわない異常なトラフィックの量を計算する。

【００２２】

例えば、監視対象機器３０１がルータやスイッチ等の中継機器である場合、その機器の

主な目的は、外部から受信したデータを別の場所へ転送することである。したがって、この監視対象機器３０１により生成されて出力されるようなデータや、この機器で終端されて廃棄されるデータや、そのデータを受信したインタフェースから送信されるようなデータは、通常は非常に少ないはずである。このようなデータが大量に発生した場合には、何らかの障害が発生したと考えられる。

【００２３】

そこで、異常トラフィック量計算装置３１４は、これらのデータの量を異常トラフィック量としてカウントし、それ以外のデータの量を正常トラフィック量としてカウントして、得られた正常／異常トラフィック量を障害判定装置３１５に転送する。

【００２４】

図５のモデルの場合、トラフィック流量分析装置３１３により推定された$x_{\alpha\beta}$のうち、x_{AA}、x_{BB}、x_{CC}、x_{A0}、x_{B0}、x_{C0}、x_{0A}、x_{0B}、およびx_{0C}が異常トラフィック量としてカウントされる。x_{AA}、x_{BB}、およびx_{CC}は、データを受信したインタフェースからそのデータが送信されるようなループトラフィックの量を表している。また、x_{A0}、x_{B0}、およびx_{C0}は、ルータ内部で廃棄されるトラフィックの量を表し、x_{0A}、x_{0B}、およびx_{0C}は、ルータ内部で生成されて出力されるトラフィックの量を表している。そこで、異常トラフィック量計算装置３１４は、これらのトラフィックの総量を計算する。

ステップ４０５：

障害判定装置３１５は、異常トラフィック量計算装置３１４が算出した正常／異常トラフィック量に基づいて障害の有無を判定する。このとき、異常トラフィックの総量が、ネットワーク管理者等が指定した所定の閾値を超えた場合に、障害が発生したものと判断する。

【００２５】

図５のモデルの場合、次式のような評価関数ｆ（Ｘ）を用いて、ルータ内部のトラフィックの総量に対する異常トラフィック量の比率が計算される。

【００２６】

【数２】

$$f(X) = \frac{\sum_{\mu} (x_{\mu 0} + x_{0\mu} + x_{\mu\mu})}{\sum_{\mu}\sum_{\nu} x_{\mu\nu} + \sum_{\mu} (x_{\mu 0} + x_{0\mu})} \qquad (5)$$

$$(\mu,\ \nu \equiv \{A,\ B,\ C\})$$

【００２７】

（５）式の右辺の分子は、異常トラフィックの総量を表す。また、（５）式の右辺の分母は、トラフィックの総量を表し、正常トラフィックの総量と異常トラフィックの総量を加算することで得られる。障害判定装置３１５は、このｆ（Ｘ）の値を所定の閾値と比較し、その値が閾値を超えれば障害が発生したものと判断する。例えば、許容可能な異常トラフィック量が全体のトラフィック量の１０％である場合、閾値は０．１に設定される。

ステップ４０６：

障害判定装置３１５は、ステップ４０５において障害が発生したと判断した場合、アラームを出力してネットワーク管理者等に障害の発生を通知する。

【００２８】

図５では３つのインタフェースを有するルータのモデルが示されているが、インタフェースの数がそれより多い場合も、同様のモデルを構築することで障害を検出することができる。

【００２９】

また、ルータ等の中継機器以外の監視対象機器３０１としては、ファイアウォールやプ

ロキシサーバ等のように、ゲートウェイとしての役割を果たす機器が考えられる。このような監視対象機器は、図６のようなモデルにより表現できる。このモデルにおいては、監視対象機器は２つのインタフェースＡおよびＢを持ち、それぞれのインタフェースにおける単位時間当たりの受信トラフィック量（y_{in-A}，y_{in-B}）と送信トラフィック量（y_{out-A}，y_{out-B}）がトラフィック流量情報として取得される。

【００３０】

また、ルータの内部には、トラフィックの終点や始点に対応する仮想的な点Ｏがあるものとし、α（$\alpha \in \{A, B, O\}$）を始点としβ（$\beta \in \{A, B, O\}$）を終点として流れるトラフィックの量は$x_{\alpha\beta}$と記されるものとする。この場合も、図５のモデルの場合と同様に、$x_{\alpha\beta}$を未知数とする連立方程式からTraffic Matrix Estimation により各$x_{\alpha\beta}$の値が推定される。

【００３１】

図７は、本発明を実施するための別のネットワーク構成の例を示している。図７のネットワーク構成において、通信ネットワーク７０１は、監視対象機器７１１、７１２、およびネットワーク監視装置７１３を含み、通信ネットワーク７０２は、監視対象機器７２１およびネットワーク監視装置７２２を含み、通信ネットワーク７０３は、監視対象機器７３１、７３２、７３３、およびネットワーク監視装置７３４を含む。

【００３２】

障害検出装置７０４は、通信ネットワーク７０１、７０２、および７０３の外部に設けられ、図８に示すように、トラフィック流量記録装置８０１、トラフィック流量分析装置８０２、異常トラフィック量計算装置８０３、および障害判定装置８０４を備える。

【００３３】

ネットワーク監視装置７１３、７２２、および７３４はそれぞれ、図９に示すように、トラフィック流量取得装置９０１およびトラフィック流量記録装置９０２を備え、各ネットワーク内の監視対象機器からトラフィック流量情報を取得して障害検出装置７０４に送信する。そして、障害検出装置７０４は、各ネットワーク監視装置から送信されたトラフィック流量情報を用いて各ネットワーク内部の障害を検出する。

【００３４】

図８のトラフィック流量記録装置８０１、トラフィック流量分析装置８０２、異常トラフィック量計算装置８０３、および障害判定装置８０４の機能は、基本的に、図３のトラフィック流量記録装置３１２、トラフィック流量分析装置３１３、異常トラフィック量計算装置３１４、および障害判定装置３１５の機能と同様である。また、図９のトラフィック流量取得装置９０１およびトラフィック流量記録装置９０２の機能は、基本的に、図３のトラフィック流量取得装置３１１およびトラフィック流量記録装置３１２の機能と同様である。

【００３５】

このようなネットワーク構成は、セキュリティ等の理由により、監視対象機器が配置されているネットワークの外部からそのネットワークの内部へのアクセスが困難な場合に、有効である。このような構成であれば、障害検出装置７０４は、それぞれのネットワーク内部に配置されているネットワーク監視装置から送られてくるトラフィック流量情報を記録すればよい。したがって、障害検出装置７０４自身がそれぞれの監視対象機器と直接通信不可能であっても、それらの監視対象機器における障害発生の有無を判断することが可能である。

【００３６】

ところで、図３および図８の障害検出装置と、図９のネットワーク監視装置は、例えば、図１０に示すような情報処理装置（コンピュータ）を用いて構成することができる。図１０の情報処理装置は、ＣＰＵ（中央処理装置）１００１、メモリ１００２、入力装置１００３、出力装置１００４、外部記憶装置１００５、媒体駆動装置１００６、ネットワーク接続装置１００７を備え、それらはバス１００８により互いに接続されている。

【００３７】

メモリ１００２は、例えば、ＲＯＭ（read only memory）、ＲＡＭ（random access memory）等を含み、処理に用いられるプログラムおよびデータを格納する。ＣＰＵ１００１は、メモリ１００２を利用してプログラムを実行することにより、必要な処理を行う。

【００３８】

図３のトラフィック流量記録装置３１２、図８のトラフィック流量記録装置８０１、および図９のトラフィック流量記録装置９０２は、メモリ１００２に対応する。また、図３のトラフィック流量取得装置３１１、トラフィック流量分析装置３１３、異常トラフィック量計算装置３１４、障害判定装置３１５、図８のトラフィック流量分析装置８０２、異常トラフィック量計算装置８０３、障害判定装置８０４、および図９のトラフィック流量取得装置９０１は、メモリ１００２に格納されたプログラムを実行することにより実現される機能に対応する。

【００３９】

入力装置１００３は、例えば、キーボード、ポインティングデバイス、タッチパネル等であり、ネットワーク管理者等のオペレータからの指示や情報の入力に用いられる。出力装置１００４は、例えば、ディスプレイ、プリンタ、スピーカ等であり、オペレータへの問い合わせ、アラーム、処理結果等の出力に用いられる。

【００４０】

外部記憶装置１００５は、例えば、磁気ディスク装置、光ディスク装置、光磁気ディスク装置、テープ装置等である。情報処理装置は、この外部記憶装置１００５に、上記プログラムおよびデータを格納しておき、必要に応じて、それらをメモリ１００２にロードして使用する。

【００４１】

媒体駆動装置１００６は、可搬記録媒体１００９を駆動し、その記録内容にアクセスする。可搬記録媒体１００９は、メモリカード、フレキシブルディスク、ＣＤ－ＲＯＭ（compact disk read only memory ）、光ディスク、光磁気ディスク等の任意のコンピュータ読み取り可能な記録媒体である。オペレータは、この可搬記録媒体１００９に上記プログラムおよびデータを格納しておき、必要に応じて、それらをメモリ１００２にロードして使用する。

【００４２】

ネットワーク接続装置１００７は、ＬＡＮ（local area network）、インターネット等の任意の通信ネットワークに接続され、通信に伴うデータ変換を行う。情報処理装置は、必要に応じて、上記プログラムおよびデータを外部の装置からネットワーク接続装置１００７を介して受け取り、それらをメモリ１００２にロードして使用する。

【００４３】

図１１は、図１０の情報処理装置にプログラムおよびデータを供給することのできるコンピュータ読み取り可能な記録媒体を示している。可搬記録媒体１００９やサーバ１１０１のデータベース１１０３に格納されたプログラムおよびデータは、情報処理装置１１０２のメモリ１００２にロードされる。サーバ１１０１は、そのプログラムおよびデータを搬送する搬送信号を生成し、ネットワーク上の任意の伝送媒体を介して情報処理装置１１０２に送信する。ＣＰＵ１００１は、そのデータを用いてそのプログラムを実行し、必要な処理を行う。

【００４４】

（付記１）　複数の通信インタフェースを有し通信ネットワーク内に配置された監視対象機器から得られる情報に基づいて、ネットワーク障害を検出する障害検出装置であって、

前記監視対象機器の各インタフェースにおける受信トラフィック量と送信トラフィック量を表すトラフィック流量情報を格納する格納手段と、

前記トラフィック流量情報を用いて、前記監視対象機器の内部における複数のトラフィックのうち異常なトラフィックの流量を計算し、得られた流量を異常トラフィック量として出力する計算手段と、

前記異常トラフィック量を用いて前記ネットワーク障害が発生したか否かを判定し、判定結果を出力する判定手段と
を備えることを特徴とする障害検出装置。

【００４５】

（付記２）　複数の通信インタフェースを有し通信ネットワーク内に配置された監視対象機器から得られる情報に基づいて、ネットワーク障害を検出するコンピュータのためのプログラムであって、

前記コンピュータの格納手段から、前記監視対象機器の各インタフェースにおける受信トラフィック量と送信トラフィック量を表すトラフィック流量情報を取り出し、

前記トラフィック流量情報を用いて、前記監視対象機器の内部における複数のトラフィックのうち異常なトラフィックの流量を計算し、

得られた流量を異常トラフィック量として用いて前記ネットワーク障害が発生したか否かを判定する
処理を前記コンピュータに実行させることを特徴とするプログラム。

【００４６】

（付記３）　前記監視対象機器により生成されて出力されるデータのトラフィック量と、該監視対象機器により廃棄されるデータのトラフィック量と、該監視対象機器のインタフェースにより受信された後に同じインタフェースから送信されるデータのトラフィック量のうち少なくとも１つのトラフィック量を、前記異常トラフィック量として計算する処理を前記コンピュータに実行させることを特徴とする付記２記載のプログラム。

【００４７】

（付記４）　前記監視対象機器の内部におけるトラフィックの総量に対する前記異常トラフィック量の比率を求め、該異常トラフィック量の比率が所定の閾値より大きい場合に前記ネットワーク障害が発生したと判定する処理を前記コンピュータに実行させることを特徴とする付記２記載のプログラム。

【００４８】

（付記５）　前記監視対象機器の内部にトラフィックの終点および始点を表す仮想点を設け、該監視対象機器の内部において各インタフェースを始点とし他のインタフェースを終点とする第１のトラフィックの流量と、各インタフェースを始点とし該仮想点を終点とする第２のトラフィックの流量と、該仮想点を始点とし各インタフェースを終点とする第３のトラフィックの流量と、該監視対象機器の内部において各インタフェースを始点とし同じインタフェースを終点とする第４のトラフィックの流量を計算し、該第２、第３、および第４のトラフィックの流量の総量を前記異常トラフィック量として計算する処理を前記コンピュータに実行させることを特徴とする付記２記載のプログラム。

【００４９】

（付記６）　前記第１、第２、第３、および第４のトラフィックの流量の総量に対する前記異常トラフィック量の比率を求め、該異常トラフィック量の比率が所定の閾値より大きい場合に前記ネットワーク障害が発生したと判定する処理を前記コンピュータに実行させることを特徴とする付記５記載のプログラム。

【００５０】

（付記７）　前記トラフィック流量情報から前記第１、第２、第３、および第４のトラフィックの流量を推定する処理を前記コンピュータに実行させることを特徴とする付記５記載のプログラム。

【００５１】

（付記８）　前記監視対象機器から前記トラフィック流量情報を取得して前記格納手段に格納する処理を前記コンピュータにさらに実行させることを特徴とする付記２記載のプログラム。

【００５２】

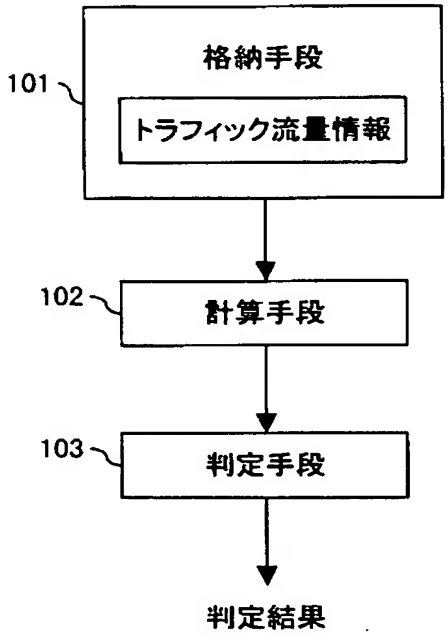
（付記９）　前記ネットワーク障害が発生したと判定したとき、アラームを出力する処理を前記コンピュータにさらに実行させることを特徴とする付記２記載のプログラム。

【００５３】
（付記１０）　複数の通信インタフェースを有し通信ネットワーク内に配置された監視対象機器から得られる情報に基づいて、ネットワーク障害を検出するコンピュータのためのプログラムを記録した記録媒体であって、
前記プログラムは、
前記コンピュータの格納手段から、前記監視対象機器の各インタフェースにおける受信トラフィック量と送信トラフィック量を表すトラフィック流量情報を取り出し、
前記トラフィック流量情報を用いて、前記監視対象機器の内部における複数のトラフィックのうち異常なトラフィックの流量を計算し、
得られた流量を異常トラフィック量として用いて前記ネットワーク障害が発生したか否かを判定する
処理を前記コンピュータに実行させることを特徴とするコンピュータ読み取り可能な記録媒体。
【００５４】
（付記１１）　複数の通信インタフェースを有し通信ネットワーク内に配置された監視対象機器から得られる情報に基づいて、ネットワーク障害を検出するコンピュータのためのプログラムを搬送する搬送信号であって、
前記プログラムは、
前記コンピュータの格納手段から、前記監視対象機器の各インタフェースにおける受信トラフィック量と送信トラフィック量を表すトラフィック流量情報を取り出し、
前記トラフィック流量情報を用いて、前記監視対象機器の内部における複数のトラフィックのうち異常なトラフィックの流量を計算し、
得られた流量を異常トラフィック量として用いて前記ネットワーク障害が発生したか否かを判定する
処理を前記コンピュータに実行させることを特徴とする搬送信号。
【００５５】
（付記１２）　複数の通信インタフェースを有し通信ネットワーク内に配置された監視対象機器から得られる情報に基づいて、ネットワーク障害を検出する障害検出方法であって、
前記監視対象機器の各インタフェースにおける受信トラフィック量と送信トラフィック量を表すトラフィック流量情報を用いて、前記監視対象機器の内部における複数のトラフィックのうち異常なトラフィックの流量を計算し、
得られた流量を異常トラフィック量として用いて前記ネットワーク障害が発生したか否かを判定する
ことを特徴とする障害検出方法。
【図面の簡単な説明】
【００５６】
【図１】本発明の障害検出装置の原理図である。
【図２】第１のネットワーク構成を示す図である。
【図３】第１の障害検出装置の構成図である。
【図４】障害検出処理のフローチャートである。
【図５】第１の監視対象機器のモデルを示す図である。
【図６】第２の監視対象機器のモデルを示す図である。
【図７】第２のネットワーク構成を示す図である。
【図８】第２の障害検出装置の構成図である。
【図９】ネットワーク監視装置の構成図である。
【図１０】情報処理装置の構成図である。
【図１１】記録媒体を示す図である。
【符号の説明】
【００５７】

１０１　格納手段
１０２　計算手段
１０３　判定手段
２０１、７０４　障害検出装置
２０２、２０３、２０４、２０５、２０６、２０７、３０１、７１１、７１２、７２１、７３１、７３２、７３３　監視対象機器
７１３、７２２、７３４　ネットワーク監視装置
３１１、９０１　トラフィック流量取得装置
３１２、８０１、９０２　トラフィック流量記録装置
３１３、８０２　トラフィック流量分析装置
３１４、８０３　異常トラフィック量計算装置
３１５、８０４　障害判定装置
１００１　ＣＰＵ
１００２　メモリ
１００３　入力装置
１００４　出力装置
１００５　外部記憶装置
１００６　媒体駆動装置
１００７　ネットワーク接続装置
１００８　バス
１００９　可搬記録媒体
１１０１　サーバ
１１０２　情報処理装置
１１０３　データベース

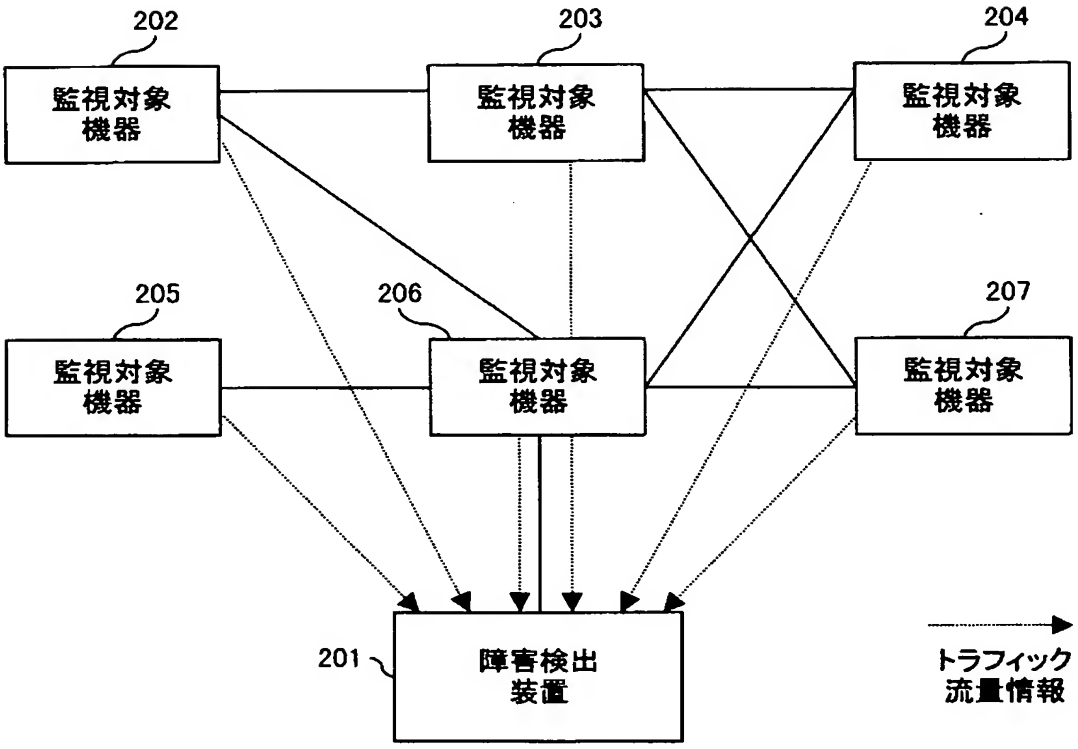
【書類名】図面
【図１】

本発明の障害検出装置の原理図



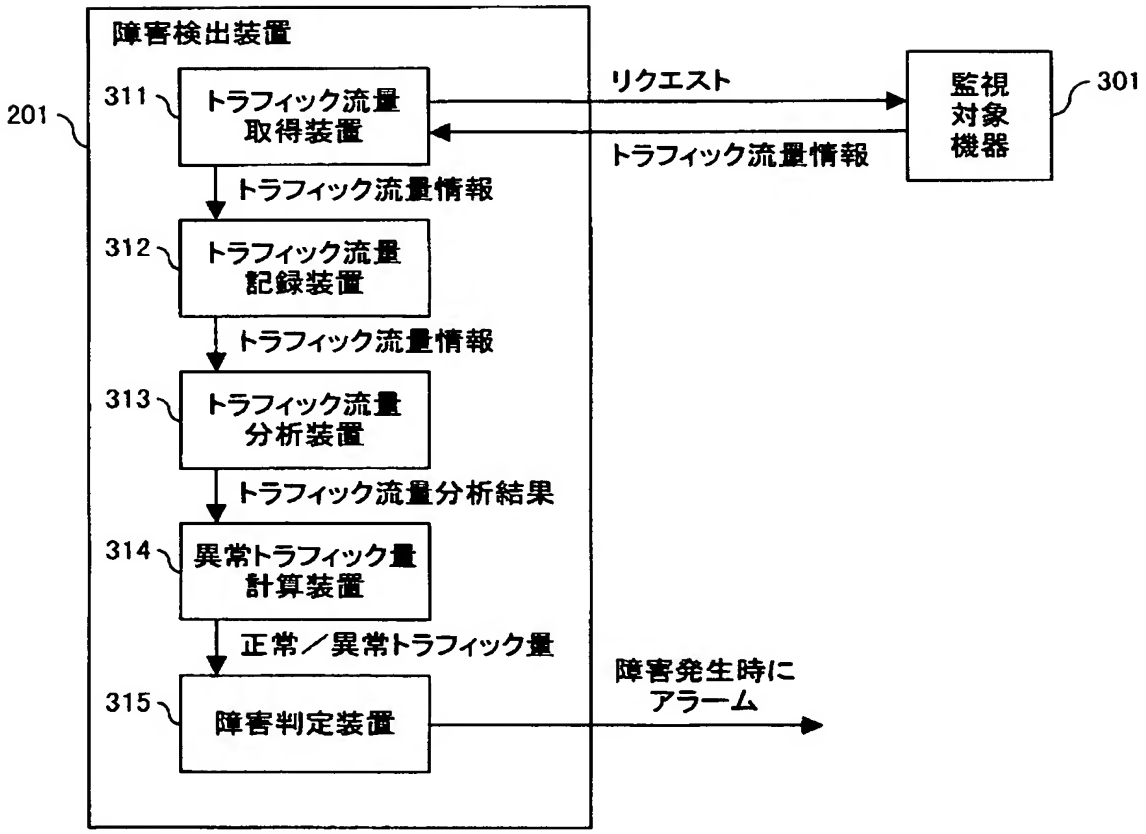
【図２】

第１のネットワーク構成を示す図



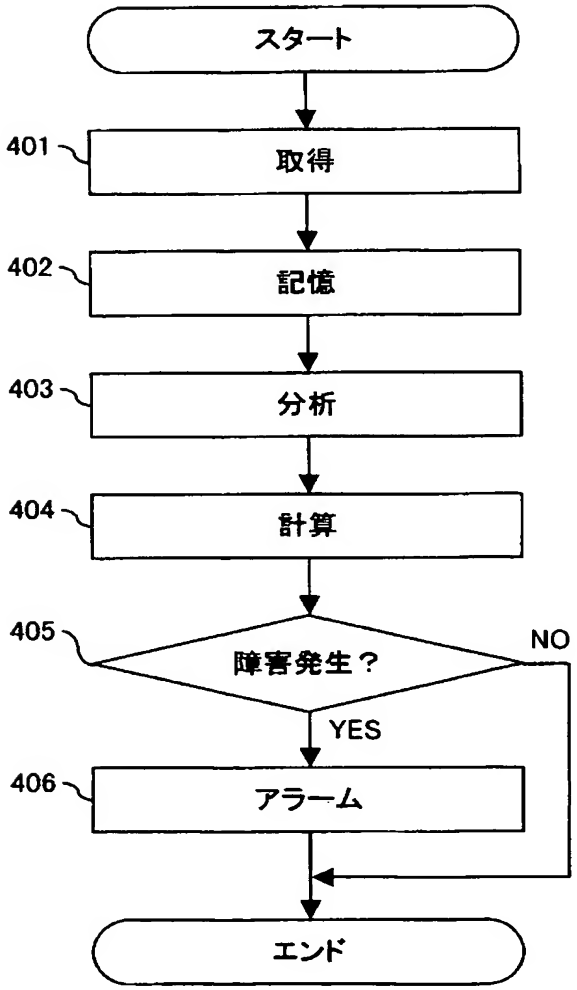
【図３】

第１の障害検出装置の構成図



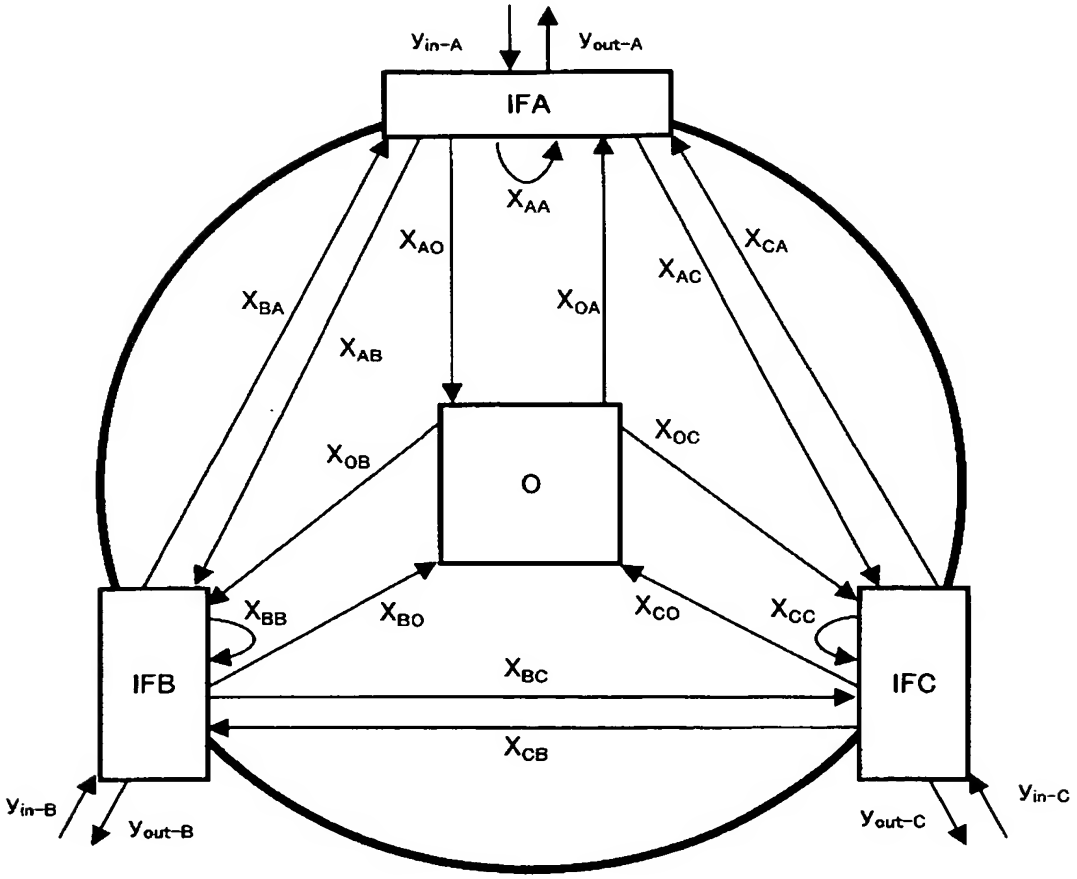
【図４】

障害検出処理のフローチャート



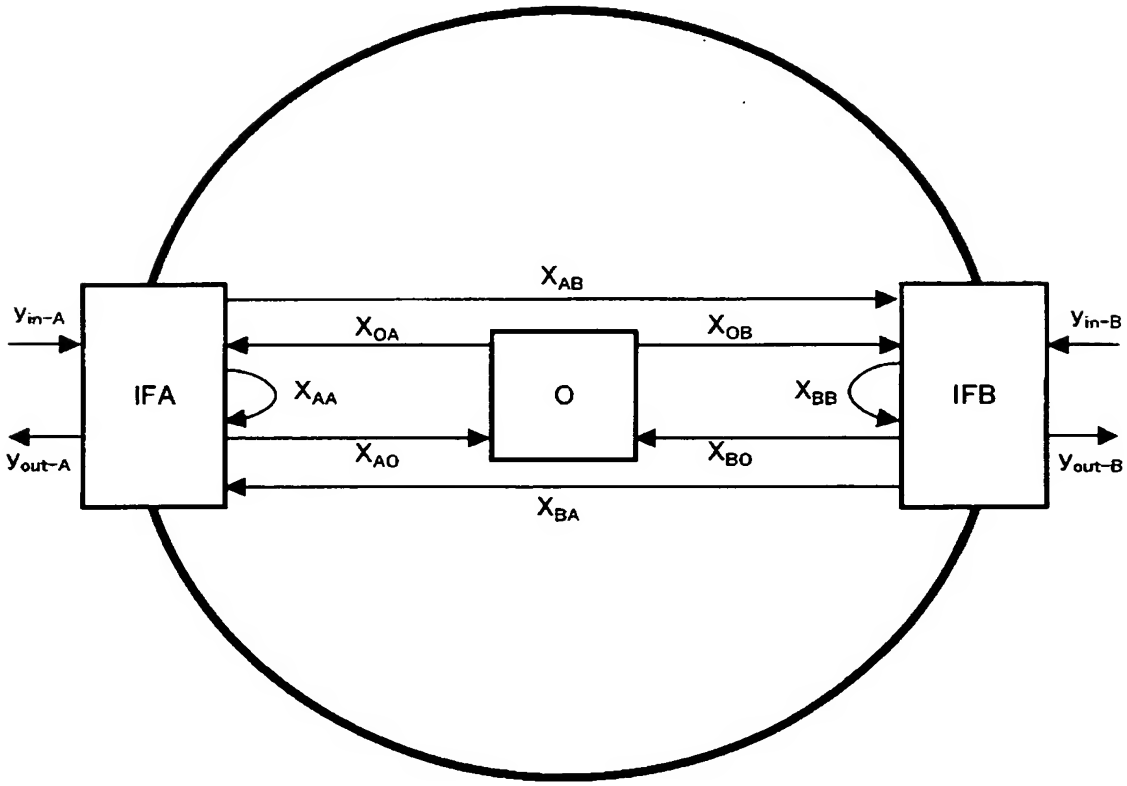
【図５】

第1の監視対象機器のモデルを示す図



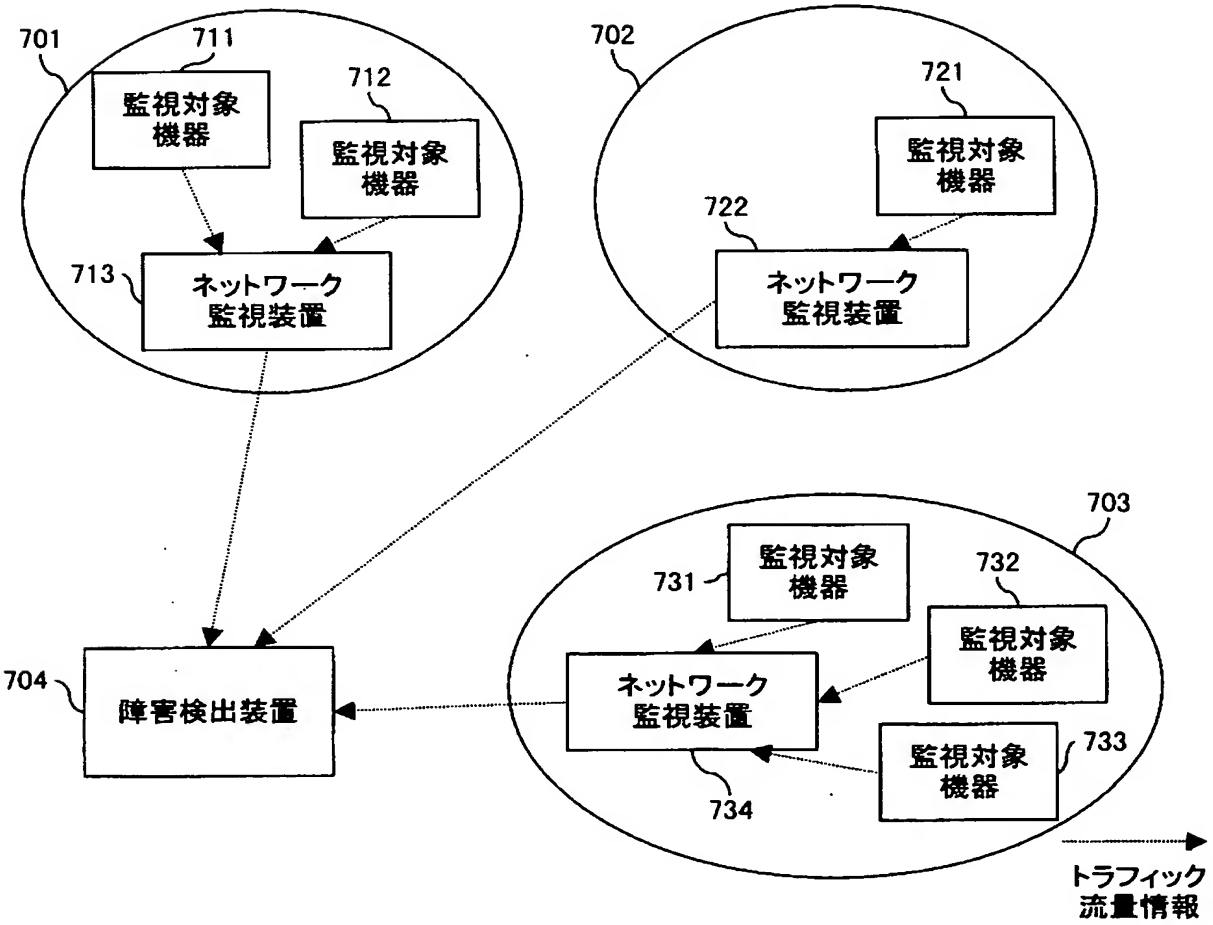
【図６】

第2の監視対象機器のモデルを示す図



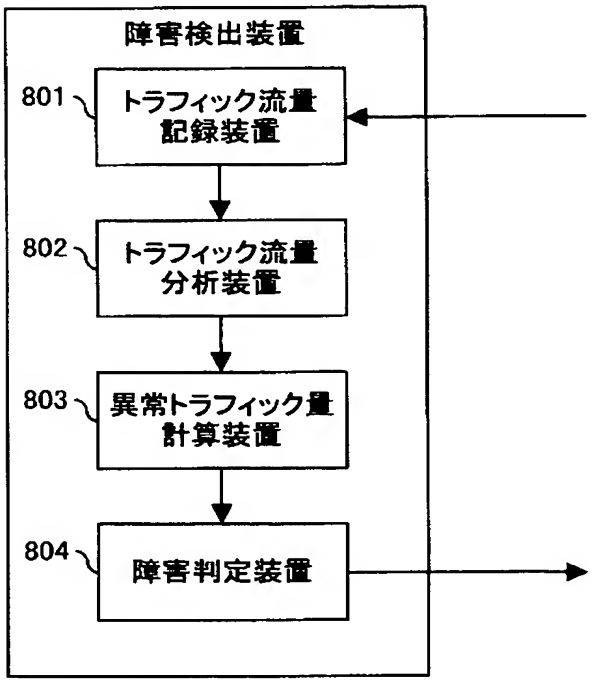
【図７】

第2のネットワーク構成を示す図



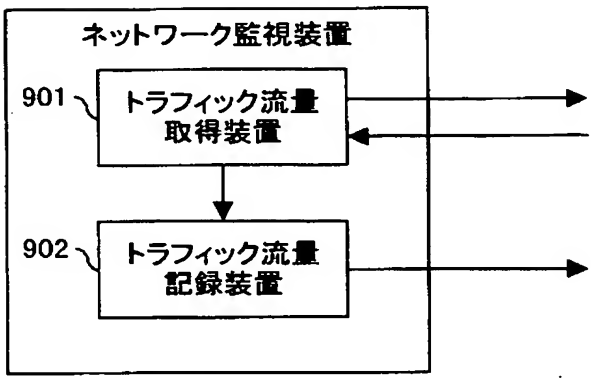
【図８】

第2の障害検出装置の構成図



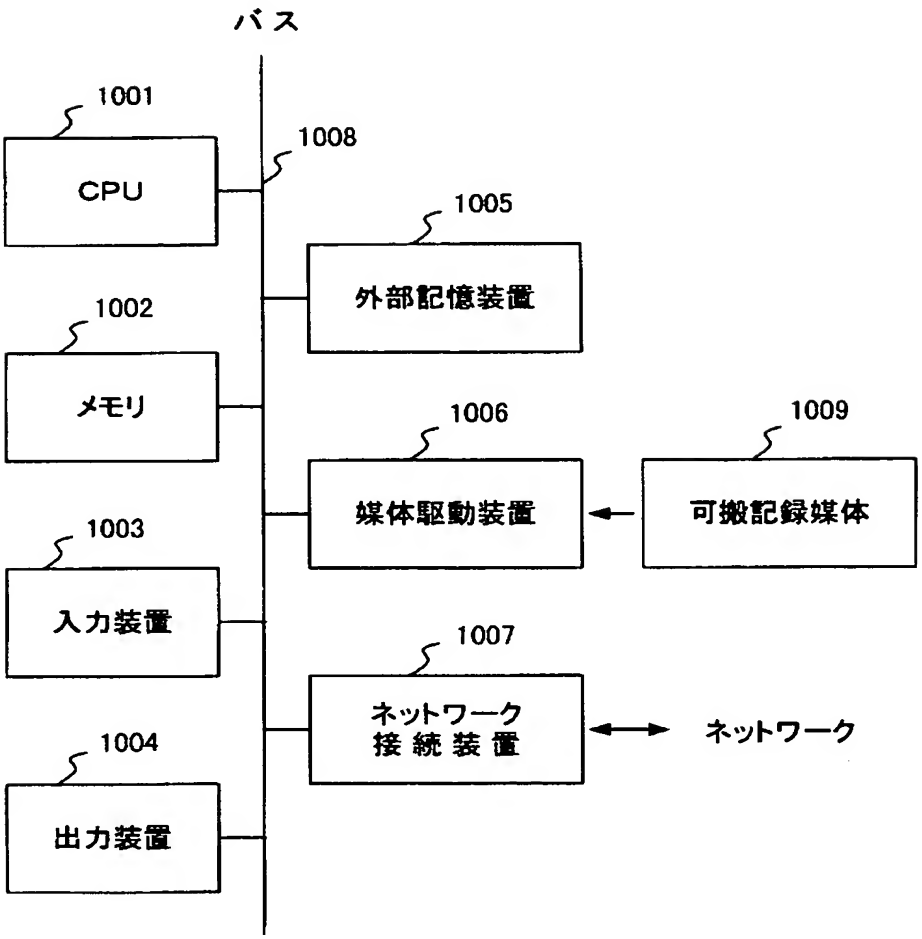
【図９】

ネットワーク監視装置の構成図



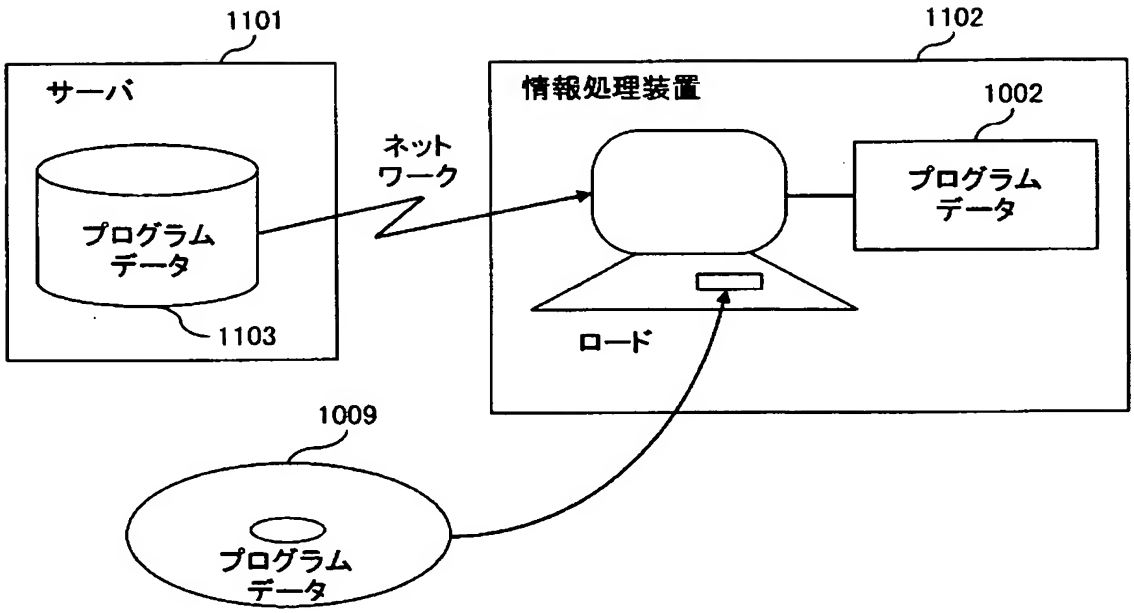
【図１０】

情報処理装置の構成図



【図１１】

記録媒体を示す図



【書類名】要約書
【要約】
【課題】　通信ネットワーク内で発生する障害を、その影響が比較的小さい早期のうちに低コストで検出する。
【解決手段】　障害検出装置２０１は、通信ネットワーク内に配置された各監視対象機器から、その機器の各インタフェースにおける受信トラフィック量と送信トラフィック量を表すトラフィック流量情報を取得する。そして、監視対象機器の内部における複数のトラフィックのうち異常なトラフィックの流量を計算し、得られた流量を用いてネットワーク障害が発生したか否かを判定する。
【選択図】　図２

特願２００３－２９６７６８

出　願　人　履　歴　情　報

識別番号　　［０００００５２２３］

１．変更年月日　　１９９６年　３月２６日
［変更理由］　　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社